#23

Docket No.: 826.1377

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re the Application of:

Hironobu KITAJIMA et al.

Serial No. 08/814,409 Group Art Unit: 2132

Confirmation No. 4623

Filed: March 11, 1997 Examiner: D. Meislahn

For: ENCRYPTING/DECRYPTING SYSTEM WITH PROGRAMMABLE LOGIC DEVICE/UNIT AND METHOD THEREOF

APPEAL BRIEF

CERTIFICATE UNDER 37 CFR 1.8(a)

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner of Patents and Trademarks, Washington, D.C. 20231
on 2/13/ ,2002,
STAAS & HALSEY LLP
By: Richard A. Dollinger
Date : 2/13/02

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

I. Real Party in Interest

The inventors Hironobu Kitajima and Shunsuke Fueki assigned all rights in the subject application to Fujitsu Limited on February 24, 1997 according to the Assignment submitted for recordation on March 11, 1997 and recorded at reel 8439, frames 259-260. Therefore, the real party in interest is Fujitsu Limited.

II. Related Appeals and Interferences

There are no related appeals or interferences known to Appellants, Appellants' legal representatives or the Assignee, Fujitsu Limited, which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. Status of Claims

Claims 1-4, 6-13 and 15-31 are pending in the application, claims 1-4, 6-13 and 15-22 stand rejected under 35 USC § 103(a) and claims 23-31 stand rejected under 35 USC § 102(b).

IV. Status of Amendments

No Amendment has been filed since the final Office Action was mailed on August 13, 2001, indicating that the Amendment filed May 29, 2001 had been entered.

V. Summary of the Invention

The present invention is directed to a high-speed encrypting/decrypting apparatus. To obtain high-speed performance, a programmable logic device (PLD) 30, such as a field programmable gate array (FPGA) 13 (Fig 3) or an application specific integrated circuit (ASIC), is used to implement encryption/decryption specifications (page 10, line 13 to page 11, line 3 and page 13, lines 5-10). Fig. 4 provides a functional block diagram of the invention and also includes the hardware blocks of host CPU 21, external unit or network 22 and PLD 30, while Fig. 5 is a structural block diagram that includes CPU 31 corresponding to CPU 21 in Fig. 4 (page 16, line 16) and network connecting unit 37 that provides the connection to external unit or network 22 shown in Fig. 4 (page 14, line 24 to page 15, line 1 and page 17, line 23 to page 18, line 4). CPU 21/31 controls changes in the structure of PLD 30 to implement changes in the encryption/decryption specifications in accordance with change data received via network connecting unit 37 (page 11, lines 4-12; page 14, line 17 to page 15, line 1 and page 16, lines 16-20). Examples of the types of changes that occur are "pin numbers and functions (logics) of the programmable logic device/unit 30 ... [as] described in the hardware description language" (page 15, lines 8-10).

During operation, the programmable logic device (PLD) 30 is used to encrypt or decrypt data in accordance with, e.g., data encryption standard (DES) or Rived-Shamir-Adleman (RSA) algorithms, implemented using adders, registers, counters, function generators and logic circuits in PLD 30 (page 18, line 5 to page 19, line 3) that are specified by a mapping data object 28 composed of a bit sequence of binary data that represents the positions of gates and lines in PLD 30 (page 15, lines 16-19). The mapping data object 28 is generated by CPU 21/31 based on a command received from network 22 which specifies an encrypting/decrypting algorithm file 24 written in hardware description language that is compiled using a basic logic hardware description language library 26 (page 14, line 17 to page line 15; Fig 4) stored in external storing unit 35 which may be a magnetic, optical or magneto-optic disc unit (page 17, lines 5-12 and page 18, lines 5-14). Configuration unit 29 in Fig. 4 represents the writing of the binary data in mapping data object 28 into PLD 30 by a program executed by CPU 21/31 (page 15, line 23 to page 16, line 7).

There are many variations of how encryption/decryption algorithms are implemented, depending on the length of the keys and size of data blocks, etc. The specifics of the algorithm performed by the present invention may be changed automatically by CPU 21/31 in response to setup data supplied from outside the device via network connecting unit 37 (page 21, line 24 to page 22, line 2). If the encrypting/decrypting algorithm file 24 to be used is not stored in database 23, a new mapping data object 28 (page 22, line 13) or a new hardware description language library 26 may be downloaded (page 22, lines 15-18).

VI. Issue

At issue on this appeal is whether the prior art teaches or suggests an encrypting/decrypting device that includes components within an enclosure capable of changing an encryption/decryption algorithm implemented in hardware by a programmable logic device automatically or in response to a simple setup command.

VII. Grouping of Claims

Independent claims 1, 10 and 19-22 and dependent claims 8 and 17 stand or fall together. Dependent claims 2 and 11, 3 and 12, and 4 and 13 may stand with claims 1 and 10, or may stand or fall separately for each pair of claims. Dependent claims 6 and 15 may stand with claims 1 and 10, or stand or fall separately from each other and the other claims. Dependent claims 7 and 16 may stand with claims 1 and 10, or stand or fall together. Dependent claims 9 and 18 may stand with claims 1 and 10, or stand or fall together. Independent claims 23-29 stand or fall together and claims 30 and 31 stand or fall together.

VIII. Argument

Claims 1-4, 6-13 and 15-22 stand rejected under 35 USC § 103(a) and claims 23-31 stand rejected under 35 USC § 102(b) with all rejections relying on U.S. Patent 4,972,478 to Dabbish as the primary or sole reference. As discussed in several of the responses filed during prosecution of this application, Dabbish '478 does not make even the broadest claims obvious when taken alone, because it does not teach how to reprogram the crypto cores 100, 101 in the device disclosed therein. A related patent, U.S. Patent 4,914,697 to Dabbish et al. must be referenced to discover how this is done. Dabbish et al. '697 states that "an external device such as a microprocessor controlled computer is coupled to the address and data bus ports and is utilized to program the internal gate configurations of each EEPAL" (column 2, lines 64-67) after installation of the EEPAL.

There is no suggestion in Dabbish '478 or Dabbish et al. '697 of "automatically generating change data for changing the encrypting (or decrypting) specification" (line 6 of claims 23 and 24) or the similar limitations recited at lines 4-6 of claim 25 and the last two lines of claims 26-29. The discussion of reprogramming of the cipher algorithm at column 1, lines 51-67 of Dabbish '478 which is cited on page 3 of the August 13, 2001 Office Action, does not suggest any kind of automatic operation as recited in claims 23-29 and column 3, lines 44-46 of Dabbish '478 merely states that decryption is similar.

Furthermore, even when Dabbish et al. '697 is substituted for Dabbish '478, there is not even a suggestion of an encrypting or decrypting unit "in which circuit connections for encrypting (decrypting) data can be changed in response (corresponding) to an external command" (lines 3-4 of claims 30 and 31). As indicated in the quotation above from Dabbish et al. '697, there is much more than a "command" supplied from outside of, i.e., from a location "external" to, the device taught by Dabbish '478 and Dabbish et al. '697. For the reasons set forth above, it is submitted that claims 23-31 are not even obvious, let alone anticipated by Dabbish '478 or Dabbish et al. '697.

The rejection of claims 1-4, 6-13 and 15-22 is based on the combination of Dabbish '478 in view of U.S. Patent 5,499,192 to Knapp et al. and the Microsoft Press Computer Dictionary, 3rd ed. (hereafter MS Computer Dictionary). As discussed in the responses to the January 26, and August 13, 2001 Office Actions, the addition of Knapp et al. and the MS Computer Dictionary to Dabbish '478 does not teach or suggest a device enclosing all of the components recited in independent claims 1, 10 and 19-22. The MS Computer Dictionary merely provides a definition of object-oriented design and it is unclear what one of ordinary skill would have learned from this definition that would suggest anything relevant to the invention.

The cited portions of Knapp et al. disclose the use of libraries of high-level functions to simplify programming of FPGA, programmable logic array (PLA) and programmable array logic (PAL) devices. However, as discussed in the Request for Reconsideration filed November 13, 2001, there is no indication of what in the device taught by Dabbish '478 could be modified using the teachings of Knapp et al. to perform the operations of the mapping data generating unit recited in claim 1 and the similar components recited in claims 10 and 19-22. Claim 1, for example, requires that something inside an enclosure reads "change data for changing at least one of the encrypting specifications in accordance with predetermined criteria received from" (claim 1, lines 8-9) outside the encrypting apparatus and generates "a mapping data object representing the structure of the encrypting circuit" (claim 1, lines 10-11). Nothing has been cited to suggest why one of ordinary skill in the art would modify the internal components of the circuit taught by Dabbish '478 to include reading change data and generating an object representing the structure of the encrypting circuit.

As discussed in the April 10, 2000 Amendment, the ability to automatically change circuit structure enables the present invention to provide the benefit of fast and flexible encryption/decryption. Specifically, the present invention provides the benefit of a system that can apply many different algorithms to blocks of data that vary in length with encryption keys that vary in length and which does not require the user to be knowledgeable in encryption algorithms, nor does it require an external computer that has been programmed with encryption/decryption algorithms. For the reasons set forth above and in the responses filed previously, it is submitted that claims 1, 10 and 19-22, as well as claims 2-9, 11-13 and 15-18 which depend from claims 1 and 10, patentably distinguish over the prior art used to reject the claims.

Many of the dependent claims add additional distinctions over the prior art used to reject the claims. As discussed in the Request for Reconsideration filed November 13, 2001, claims 2-4 and 11-13 add details regarding operations performed by the mapping data generating unit. It is unclear why one of ordinary skill in the art would find it obvious to modify any internal component of the circuit taught by Dabbish '478 to perform the operations taught by Knapp et al. Therefore, it is submitted that claims 2-4 and 11-13 further patentably distinguish over the prior art due to the details recited therein.

As also discussed in the Request for Reconsideration filed November 13, 2001, nothing has been cited in the prior art suggesting that data either received or transmitted by EPE 105 is "encrypted change data" (claim 6, line 2), or for that matter "decrypted change data" (claim 15, line 2). Since the EPE 105 and internal components of the cryptographic circuit 10 are under the control of the person programming the unit, there would be no need for encryption (or decryption) of data transmitted by EPE 105 to the internal components of circuit 10. Furthermore, there is no suggestion in Dabbish '478 of any change data being transmitted over communication circuitry 104 and therefore, there is no need to encrypt (or decrypt) any change data. For the above reasons, it is submitted that claims 6 and 15 further patentably distinguish over the prior art cited in rejecting the claims.

Furthermore, claims 7 and 16 recite that the automatic changes occur "periodically" (e.g., claim 7, line 2). The August 13, 2001 Office Action relies on "official notice" to supply this missing teaching from the cited prior art. Even if it is obvious to make periodic changes to a circuit used for pay television systems, it is unclear why one of ordinary skill in the art would apply this technique to the circuit taught by Dabbish '478 as modified by Knapp et al., particularly when there is no suggestion in the cited prior art of a system that would be capable of making changes automatically. Therefore, it is submitted that claims 7 and 16 further patentably distinguish over the prior art cited in rejecting the claims.

Finally, claims 9 and 18 recite that the encrypting/decrypting specifications change with respect "to at least one of a communication path of data to be encrypted (decrypted), a degree of security thereof, and a process speed" (lines 2-3 of claims 9 and 18). Even if U.S. Patent 5,345,508 to Lynn et al. fully teaches changing encryption and decryption specifications as recited in claims 9 and 18, it is unclear why one of ordinary skill in the art would have been motivated to modify Dabbish '478 to make such changes "automatically" as recited in claims 1 and 10. In other words, the addition of Lynn et al. to Dabbish '478 is merely an aggregation that does not suggest the invention as recited in claims 9 and 18. Therefore, it is submitted that claims 9 and 18 further patentably distinguish over the prior art cited in rejecting the claims.

Summary of Arguments

For the reasons set forth above and in the Amendments filed during prosecution of the application, it is submitted that claims 1-4, 6-13 and 15-31 patentably distinguish over the prior art cited in rejecting the claims. Thus, it is respectfully submitted that the Examiner's final rejection of the claims is without support and, therefore, erroneous. Accordingly, the Board of Patent Appeals and Interferences is respectfully urged to so find and to reverse the Examiner's final rejection.

The required fee in the amount of $320 is attached. If any additional fees are required, please charge same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: 2/13/02

By: Richard A. Gollhofer
Richard A. Gollhofer
Registration No. 31,106

700 Eleventh Street, NW, Suite 500
Washington, D.C. 20001
(202) 434-1500

IX. Appendix

1. An encrypting apparatus connectable via a communication network to a remote computer disposed at a remote place, comprising:

a circuit unit, having at least one programmable logic device, to form an encrypting circuit with the programmable logic device corresponding to given encrypting specifications;

a network connecting unit to connect said encrypting apparatus to the communication network;

a mapping data generating unit to read change data for changing at least one of the encrypting specifications in accordance with predetermined criteria received from the remote computer via the communication network, and to generate a mapping data object representing the structure of the encrypting circuit;

a changing unit, coupled to said circuit unit and said change data generating unit, to change automatically a structure of the encrypting circuit corresponding to the mapping data object by changing a circuit structure of the programmable logic device without removal from said encrypting apparatus; and

an enclosure substantially surrounding said circuit unit, said network connecting unit, said mapping data generating unit and said changing unit.

2. The encrypting apparatus as set forth in claim 1,

wherein said changing unit includes a configuration unit to write the mapping data object to the programmable logic device,

wherein said mapping data generating unit reads an existing mapping data object, and

wherein said configuration unit writes the existing mapping data object.

3. The encrypting apparatus as set forth in claim 1,

wherein said mapping data generating unit includes a compiler unit to generate the mapping data object by compiling a library written in a hardware description language,

wherein said changing unit includes a configuration unit to write the mapping data object to the programmable logic device, and wherein said mapping data generating unit reads the change data from an existing library, compiles the existing library to obtain the mapping data object, and changes the encrypting circuit using the mapping data object.

4. The encrypting apparatus as set forth in claim 1,

wherein said mapping data generating unit includes:

a database unit to store an encrypting algorithm file having a predetermined encrypting algorithm, and

a compiler unit to generate a mapping data object by compiling a library written in a hardware description language,

wherein said changing unit includes a configuration unit for writing the mapping data object to the programmable logic device; and

wherein said mapping data generating unit receives the change data from outside said encrypting apparatus, retrieves a relevant encrypting algorithm file and changes the encrypting circuit with the library in the relevant encrypting algorithm file, corresponding to setup data given as the change data.

6. The encrypting apparatus as set forth in claim 1, wherein said network connecting unit receives encrypted change data from the communication network, and said mapping data generating unit generates the encrypting circuit using the encrypted change data.

7. The encrypting apparatus as set forth in claim 1, wherein said changing unit periodically updates the encrypting specifications.

8. The encrypting apparatus as set forth in claim 1, wherein said changing unit updates the encrypting specifications corresponding to an external command.

5
~~9.~~ The encrypting apparatus as set forth in claim 1, wherein said changing unit changes the encrypting specifications corresponding to at least one of a communication path of data to be encrypted, a degree of security thereof, and a process speed required therefor.

10. A decrypting apparatus connectable via a communication network to a remote computer disposed at a remote place, comprising:

a circuit unit, having at least one programmable logic device, to form a decrypting circuit with the programmable logic device corresponding to given decrypting specifications;

a network connecting unit to connect said decrypting apparatus to the communication network;

a mapping data generating unit to read change data for changing at least one of the decrypting specifications in accordance with predetermined criteria received from the remote computer via the communication network, and to generate a mapping data object representing the structure of the decrypting circuit;

a changing unit, coupled to said circuit unit and said change data generating unit, to change automatically a structure of the decrypting circuit corresponding to the mapping data by changing a circuit structure of the programmable logic device without removal from said decrypting apparatus; and

an enclosure substantially surrounding said circuit unit, said mapping data generating unit and said changing unit.

11. The decrypting apparatus as set forth in claim 10,

wherein said changing unit includes a configuration unit to write the mapping data object to the programmable logic device,

wherein said mapping data generating unit reads an existing mapping data object, and

wherein said configuration unit writes the existing mapping data object.

12. The decrypting apparatus as set forth in claim 10,

wherein said mapping data generating unit includes a compiler unit to generate a mapping data object by compiling a library written in a hardware description language, and

wherein said changing unit includes a configuration unit to write the mapping data object to the programmable logic device, and

wherein said mapping data generating unit reads the change data from an existing library, compiles the existing library to obtain the mapping data object, and changes the decrypting circuit using the mapping data object.

13. The decrypting apparatus as set forth in claim 10,

wherein said mapping data generating unit includes:

a database unit to store a decrypting algorithm file having a predetermined decrypting algorithm, and

a compiler unit to generate a mapping data object by compiling a library written in a hardware description language,

wherein said changing unit includes a configuration unit for writing the mapping data object to the programmable logic device; and

wherein said mapping data generating unit receives the change data from outside said decrypting apparatus, retrieves a relevant decrypting algorithm file and changes the decrypting circuit with the library in the relevant decrypting algorithm file, corresponding to setup data given as the change data.

15. The decrypting apparatus as set forth in claim 10,

wherein said network connecting unit receives decrypted change data from the communication network, and

wherein said mapping data generating unit changes the decrypting circuit corresponding to the decrypted change data.

16. The decrypting apparatus as set forth in claim 10, wherein said changing unit periodically updates the decrypting specifications.

17. The decrypting apparatus as set forth in claim 10, wherein said changing unit updates the decrypting specifications corresponding to an external command.

18. The decrypting apparatus as set forth in claim 10, wherein said changing unit changes the decrypting specifications corresponding to at least one of a communication path of data to be decrypted, a degree of security thereof, and a process speed required therefor.

19. A signal processing apparatus connectable via a communication network to a remote computer disposed at a remote place, comprising:

circuit means, having at least one programmable logic device, for forming a circuit corresponding to given specifications;

mapping data generating means for reading change data from the remote computer via the communication network, for changing the specifications of the circuit in accordance with predetermined criteria and for generating a mapping data object representing the structure of the circuit, the change data representing one of encrypting specifications or decrypting specifications;

changing means for automatically changing a structure of the circuit corresponding to the mapping data object; and

an enclosure substantially surrounding said circuit means, said mapping data generating means and said changing means.

20. An encryption processing system for use with a communication system for exchanging encrypted data through a communication network connected to a remote computer at a remote location, comprising:

encrypting circuit means, having at least one programmable logic device, for forming an encrypting circuit corresponding to given encrypting specifications;

encryption mapping data generating means for reading encryption change data from the remote computer via the communication network, for changing the encrypting specifications in accordance with predetermined criteria and for generating an encryption mapping data object representing the structure of the encrypting circuit;

encryption changing means for changing the encrypting specifications and automatically changing a structure of the encrypting circuit corresponding to the encryption mapping data object;

decrypting circuit means, having at least one programmable logic device, for forming a decrypting circuit corresponding to given decrypting specifications;

decryption mapping data generating means for reading decryption change data from the remote computer via the communication network, for changing the decrypting specifications in accordance with the predetermined criteria and for generating a decryption mapping data object representing the structure of the decrypting circuit;

decryption changing means for changing the decrypting specifications and automatically changing a structure of the decrypting circuit corresponding to the decryption mapping data object; and

an enclosure substantially surrounding said encryption and decryption circuit means, said encryption and decryption mapping data generating means and said encryption and decryption changing means.

21. An encrypting apparatus connectable via a communication network to a remote computer disposed at a remote place, comprising:

encrypting means, composed of an unit of which circuit connections for encrypting data can be changed corresponding to an external command, for encrypting data;

mapping data generating means for reading change data from the remote computer via the communication network to change encrypting specifications in accordance with predetermined criteria and for generating a mapping data object representing the structure of the circuit connections;

changing means for changing the circuit connections of said encrypting means corresponding to the encrypting specifications of the encrypting algorithm only when the encrypting specifications are changed based on the mapping data object; and

an enclosure substantially surrounding said encrypting means, said mapping data generating means and said changing means.

22. A decrypting apparatus connectable via a communication network to a remote computer disposed at a remote place, comprising:

decrypting means, composed of an unit of which circuit connections for decrypting data can be changed corresponding to an external command, for decrypting data;

mapping data generating means for reading change data from the remote computer via the communication network to change decrypting specifications in accordance with predetermined criteria and for generating a mapping data object representing the structure of the circuit connections;

changing means for changing the circuit connections of said decrypting means corresponding to the decrypting specifications of the decrypting algorithm only when the decrypting specifications are changed based on the mapping data object; and

an enclosure substantially surrounding said encrypting means, said mapping data generating means and said changing means.

23. An encrypting method, comprising:

forming an encrypting circuit corresponding to given encrypting specifications with at least one programmable logic device;

reading change data from a remote computer via a communication network, for changing the encrypting specifications; and

automatically generating change data for changing the encrypting specification; and automatically changing a circuit structure of the at least one programmable logic device corresponding to the change data without removal of the at least one programmable logic device from the encrypting circuit.

24. A decrypting method, comprising:

forming a decrypting circuit corresponding to given decrypting specifications with at least one programmable logic device;

reading change data from a remote computer via a communication network, for changing the decrypting specifications;

automatically generating change data for changing the decrypting specification; and

automatically changing a circuit structure of the at least one programmable logic device corresponding to the change data without removal of the at lcast one programmable logic device from the decrypting circuit.

25. A signal processing method, comprising:

forming a circuit corresponding to given specifications with at least one programmable logic device;

automatically generating change data for changing the specifications of the circuit, the specifications representing one of encrypting specifications or decrypting specifications; and

reading the change data from a remote computer via a communication network, and automatically changing a structure of the circuit corresponding to the change data.

26. An encrypting apparatus connectable via a communication network to a remote computer disposed at a remote place, comprising:

a circuit unit, having at least one programmable logic device, to form an encrypting circuit with the programmable logic device corresponding to given encrypting specifications;

a network connecting unit to connect said encrypting apparatus to the communication network; and

a changing unit to read change data from the remote computer for changing the encrypting specifications, and automatically to change the encrypting circuit corresponding to the change data.

27. A decrypting apparatus connectable via a communication network to a remote computer disposed at a remote place, comprising:

a circuit unit, having at least one programmable logic device, to form a decrypting circuit with the programmable logic device corresponding to given decrypting specifications;

a network connecting unit to connect said decrypting apparatus to the communication network; and

a changing unit to read change data from the remote computer for changing the decrypting specifications, and automatically to change the decrypting circuit corresponding to the change data.

28. A signal processing apparatus connectable via a communication network to a remote computer disposed at a remote place, comprising:

a circuit unit, having at least one programmable logic device, for forming a circuit corresponding to given specifications;

a network connecting unit to connect said signal processing apparatus to the communication network; and

a changing unit to read change data from the remote computer for changing the specifications of the circuit, the change data representing one of encrypting specifications and decrypting specifications, and automatically to change the circuit corresponding to the change data.

29. An encryption processing system for use with a communication system for exchanging encrypted data through a communication network connected to a remote computer disposed at a remote place, comprising:

an encrypting circuit unit, having at least one programmable logic device, to form an encrypting circuit corresponding to given encrypting specifications;

an encryption changing unit to read encryption change data from the remote computer for changing the encrypting specifications, and automatically to change the encrypting circuit corresponding to the encryption change data;

a decrypting circuit unit, having at least one programmable logic device, to form a decrypting circuit corresponding to given decrypting specifications; and

a decryption changing unit to read decryption change data from the remote computer for changing the decrypting specifications, and automatically to change the decrypting circuit corresponding to the decryption change data.

18 ~~30.~~ An encrypting apparatus connectable via a communication network to a remote computer disposed at a remote place, comprising:

an encrypting unit in which circuit connections for encrypting data can be changed in response to an external command;

a network connecting unit to connect the encrypting apparatus to the communication network; and

a changing unit for changing the circuit connections of said encrypting unit corresponding to specifications of an encrypting algorithm, read from the remote computer when the specifications are changed.

9 ~~31.~~ A decrypting apparatus connectable via a communication network to a remote computer disposed at a remote place, comprising:

a decrypting unit in which circuit connections for decrypting data can be changed corresponding to an external command;

a network connecting unit to connect the decrypting apparatus to the communication network; and

a changing unit for changing the circuit connections of said decrypting unit corresponding to specifications of a decrypting algorithm, read from the computer when the specifications are changed.